SHPathPrepareForWrite

Vulnerable to TOCTOU issues

Sean Barnum, Cigital, Inc. [vita[1]]

2007-04-16

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4698 bytes

<table>
<tr><td><b>Attack Category</b></td><td><ul><li>Path spoofing or confusion problem</li></ul></td></tr>
<tr><td><b>Vulnerability Category</b></td><td><ul><li>Indeterminate File/Path</li><li>TOCTOU - Time of Check, Time of Use</li></ul></td></tr>
<tr><td><b>Software Context</b></td><td><ul><li>File Management</li><li>File Path Management</li></ul></td></tr>
<tr><td><b>Location</b></td><td></td></tr>
<tr><td><b>Description</b></td><td><p>SHPathAvailableForWrite() is vulnerable to Time Of Check/ Time Of Use (TOCTOU) attacks.</p><p>SHPathAvailableForWrite() checks to see if the path exists. This includes remounting mapped network drives, prompting for ejectable media to be reinserted, creating the paths, prompting for the media to be formatted, and providing the appropriate user interfaces, if necessary. Read/write permissions for the medium are not checked.</p><p>This function is a check-category TOCTOU function.</p></td></tr>
<tr><td><b>APIs</b></td><td><table><tr><th>Function Name</th><th>Comments</th></tr><tr><td>SHPathPrepareForWrite</td><td>check</td></tr></table></td></tr>
<tr><td><b>Method of Attack</b></td><td>TOCTOU vulnerabilities can lead to process/file interaction race conditions. An attacker can potentially alter the checked circumstances after the check and prior to the use. This may allow</td></tr>
</table>

[1] http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

<table>
<tr><td></td><td>the attacker to trick the program into doing something undesirable.</td></tr>
<tr><td><b>Exception Criteria</b></td><td></td></tr>
<tr><td><b>Solutions</b></td><td><table>
<tr><th>Solution Applicability</th><th>Solution Description</th><th>Solution Efficacy</th></tr>
<tr><td>Generally applicable</td><td>Ensure that at time of "use" the use will be safe even if the condition reported by SHPathPrepareForWrite() is no longer valid.</td><td>Effective.</td></tr>
</table></td></tr>
<tr><td><b>Signature Details</b></td><td>HRESULT
SHPathPrepareForWrite(
HWND hwnd,
IUnknown *punkEnableModless,
LPCTSTR pszPath,
DWORD dwFlags
);</td></tr>
<tr><td><b>Examples of Incorrect Code</b></td><td>TCHAR path[] =
TEXT("D:\\alpha\
\beta.txt");

if
(SUCCEEDED(SHPathPrepareForWrite(
hwnd, // handle
of parent interface
window
punkEnableModless, //
provides access to
EnableModeless method
path,
SHPPFW_IGNOREFILENAME //
supplied path includes
file name
)) {

FILE * theFile =
_tfopen(path, "w");

// The following is
a problem in multiple
respects: even if no
attack occurred,</td></tr>
</table>

<table>
<tr><td></td><td>// there is no
guarantee we had write
permission.
/* Proceed to write
file */
}</td></tr>
<tr><td><b>Examples of Corrected Code</b></td><td>TCHAR path[] =
TEXT("D:\\alpha\
\beta.txt");

if
(SUCCEEDED(SHPathPrepareForWrite(
hwnd, // handle
of parent interface
window
punkEnableModless, //
provides access to
EnableModeless method
path,
SHPPFW_IGNOREFILENAME //
supplied path includes
file name
)) {

FILE * theFile =
_tfopen(path, "w");

// Check to ensure
that we have an open
file handle
if (theFile != NULL)
{
/* Proceed to write
file */
} else {
/* handle error */
}
}</td></tr>
<tr><td><b>Source Reference</b></td><td>• http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/functions/shpathprepareforwrite.asp[2]</td></tr>
<tr><td><b>Recommended Resource</b></td><td>• MSDN reference for SHPathPrepareForWrite[3]</td></tr>
<tr><td><b>Discriminant Set</b></td><td><table><tr><td><b>Operating System</b></td><td>• Windows</td></tr><tr><td><b>Languages</b></td><td>• C
• C++</td></tr></table></td></tr>
</table>

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

[1] mailto:copyright@cigital.com